

# SECURITY CONTROLLER

Publication number: JP8257216

Publication date: 1996-10-08

Inventor: TAKEMOTO TAKATOSHI

Applicant: ACE DENKEN KK

Classification:

- International: A63F7/02; E05B49/00; A63F7/02; E05B49/00; (IPC1-7):  
A63F7/02; A63F7/02; E05B49/00; G10L3/00

- european:

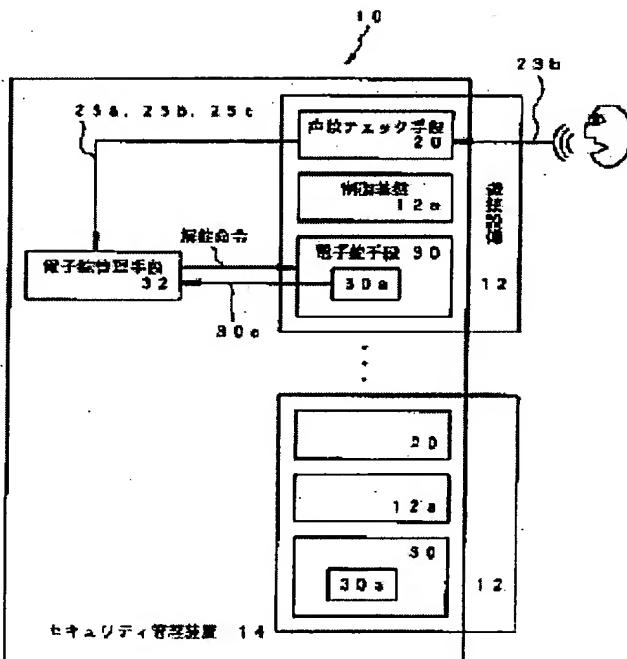
Application number: JP19950065853 19950324

Priority number(s): JP19950065853 19950324

[Report a data error here](#)

## Abstract of JP8257216

PURPOSE: To provide the security controller with which illegal access to play facilities can be prevented. CONSTITUTION: This security controller is provided with an electronic lock means 30 which is provided for each important part to be locked at respective play facilities 12,...12 constituting a playground 10 and to which inherent unlock right information 30a is previously set for each of play facilities 12,...12, a voiceprint check means 20 which set the unlock right 25a of electronic lock means 30 corresponding to a registered voiceprint in the case of matching a generated voiceprint and the registered voiceprint and generates registered voiceprint unlock right information 25b, to which the unlock right 25a is added, and an electronic lock managing means 32 for executing the unlock control of the electronic lock means 30 receiving an unlock request 25c when the peculiar unlock right information 30a is matched with the registered voiceprint unlock right information 25b.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-257216

(43)公開日 平成8年(1996)10月8日

(51)Int.Cl. <sup>6</sup>	識別記号	府内整理番号	F I	技術表示箇所
A 6 3 F 7/02	3 2 7		A 6 3 F 7/02	3 2 7 Z
	3 3 4			3 3 4
E 0 5 B 49/00			E 0 5 B 49/00	T
G 1 0 L 3/00	5 5 1		G 1 0 L 3/00	5 5 1 Z

審査請求 未請求 請求項の数3 O.L (全10頁)

(21)出願番号 特願平7-65853

(22)出願日 平成7年(1995)3月24日

(71)出願人 000127628

株式会社エース電研

東京都台東区東上野3丁目12番9号

(72)発明者 武本 孝俊

東京都台東区東上野3丁目12番9号 株式会社エース電研内

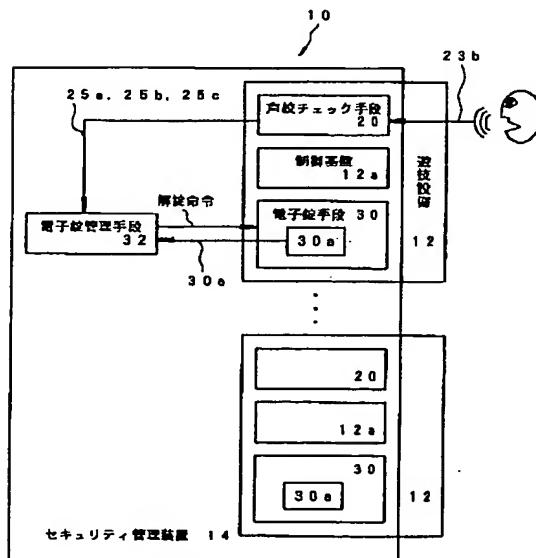
(74)代理人 弁理士 柏原 健次

(54)【発明の名称】セキュリティ管理装置

(57)【要約】

【目的】遊技設備への不正アクセスを防止できるセキュリティ管理装置を提供すること。

【構成】遊技場10を構成する各遊技設備12, …, 12の施錠すべき要所毎に設けられるとともに遊技設備12, …, 12毎に固有解錠権情報30aが各々予め設定されている電子錠手段30と、発生声紋と登録声紋とが一致した場合に登録声紋に応じて電子錠手段30の解錠権25aを設定するとともに解錠権25aを付加した登録声紋解錠権情報25bを生成する声紋チェック手段20と、固有解錠権情報30aと登録声紋解錠権情報25bとが一致したときに解錠要求25cを受けた電子錠手段30の解錠の制御を実行する電子錠管理手段32と、を備えて成る。



10…遊技場  
12a, …, 12b…制御基盤  
14…セキュリティ管理装置  
23b…発声された文字  
25a…施錠権  
25b…登録声紋解錠権情報  
25c…解錠要求  
30a…固有解錠権情報

【特許請求の範囲】

【請求項1】遊技場を構成する遊技設備への不正アクセスを防止するためのセキュリティ管理装置において、前記遊技場を構成する各遊技設備の施錠すべき要所毎に設けられるとともに当該遊技設備毎に固有解錠権情報が各々予め設定されている電子錠手段と、各遊技設備毎に設けられ、表示した文字の発声を促すとともに当該発声された文字の声紋と予め登録してある声紋との比較を実行し、当該発生声紋と当該登録声紋とが一致した場合に当該登録声紋に応じて前記電子錠手段の解錠権を設定するとともに当該解錠権を付加した登録声紋解錠権情報を生成する声紋チェック手段と、前記遊技場内に設けられ、前記電子錠手段の解錠要求である前記登録声紋解錠権情報を受けた場合に、当該解錠要求を受けた電子錠手段に予め設定されている前記固有解錠権情報と当該登録声紋解錠権情報との比較を実行し、当該固有解錠権情報と当該登録声紋解錠権情報とが一致した場合に当該解錠要求を受けた電子錠手段の解錠の制御を実行する電子錠管理手段と、を備えて成ることを特徴とするセキュリティ管理装置。

【請求項2】前記声紋チェック手段は、前記表示する文字を所定の規則に基づいて選択して発声文字データを生成する発声文字管理部と、前記発声文字データを受けて、当該発声を促す文字を表示する表示部と、前記文字の発声を受けて、前記発声された文字の声紋の声紋分析を実行して発声声紋データを生成する発声声紋管理部と、前記発声声紋データと前記登録声紋のデータとの比較を実行する声紋チェック部と、前記発生声紋データと前記登録声紋データとが一致した場合に、当該登録声紋データに応じて前記解錠権を設定するとともに当該解錠権を付加した前記登録声紋解錠権情報を生成するアクセス権付与部と、を備えて成ることを特徴とする請求項1に記載のセキュリティ管理装置。

【請求項3】前記発声文字管理部は、表示する文字をランダムに選択して前記発声文字データを生成する、ことを特徴とする請求項2に記載のセキュリティ管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、遊技場を構成する遊技設備への不正アクセスを防止するためのセキュリティ管理装置に関し、特に、遊技盤面上に遊技玉を打出して遊技玉の入賞を競うパチンコ遊技機、遊技玉の貸出しを実行するための遊技媒体貸出装置、入賞玉の計数を実行するための賞出媒体計数器等のパチンコ遊技設備、およびこれらのパチンコ遊技設備の統括的な管理を実行するた

めのパチンコ遊技場管理装置等から構成されるパチンコ遊技場における、これらの遊技設備への不正アクセスを防止するためのセキュリティ管理装置に関する。

【0002】

【従来の技術】従来の遊技場を構成する遊技設備への不正アクセスを防止するためのセキュリティ管理装置においては、鍵と鍵穴式のような機械式一致判定機構による錠手段（機械錠手段）が設けられており、保守管理用の専用鍵が準備保管されていた。

10 【0003】遊技設備（例えば、パチンコ遊技機、遊技媒体貸出装置、賞出媒体計数器等のパチンコ遊技設備、およびパチンコ遊技場管理装置）等に保守整備が必要となった際、錠手段に設けられた鍵穴に専用鍵を差し入れて、解錠し、保守整備を行うことにより、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止するためのセキュリティの管理が行われていた。

【0004】また、コンピュータ機能を中心としたセキュリティ管理装置においては、遊技設備にアクセスする場合、セキュリティ機能を一時的に解除するために、コンピュータOSが要求するLogin、またはPasswordに応答するプロセスを強制することにより、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止するためのセキュリティの管理が行われていた。LoginネームやPasswordは、機密性を保持するために定期的に変更されていた。

【0005】

【発明が解決しようとする課題】しかしながら、従来から行われている鍵と鍵穴式のような機械式一致判定機構による錠手段（機械錠手段）によるセキュリティ管理装置では、錠手段（ロック機構）毎に各々専用鍵を用意する必要があり、錠手段の種類だけ専用鍵が必要であり、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することが難しいという問題点があった。

【0006】さらに、遊技設備等に保守整備が必要となった際、合致する専用鍵を一旦探し出さなければならず、保守整備に過大な労力および時間を要し、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することが難しいという問題点があった。

【0007】さらに、専用鍵は、紛失したり、盗取されたり、模造されやすいため、多種類の専用鍵を、紛失、盗取または模造されないように保管しておくためにも過大な労力および時間を要し、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することが難しいという問題点があった。

【0008】また、Login、Password応答を強制するセキュリティ管理装置では、LoginネームやPasswordがハッキングされ易いため、容易に遊技設備内に侵入されるという問題点があった。また、定期的にLoginネームやPasswordを変更しても、機密性の保持には限界があり、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することが難しいという問題点があった。

【0009】本発明は、このような従来技術が有する問題点に着目してなされたもので、機械錠手段に代えて電子錠手段を用い、さらにLoginまたはPassword応答制御に代えて声紋チェックに基づく解錠権に応じて電子錠手段の解錠の制御を実行することにより、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止できるセキュリティ管理装置を提供することを目的としている。

#### 【0010】

【課題を解決するための手段】かかる目的を達成するための要旨とところは、以下の各項に存する。

【0011】[1] 項 遊技場（10）を構成する遊技設備（12, …, 12）への不正アクセスを防止するためのセキュリティ管理装置において、前記遊技場（10）を構成する各遊技設備（12, …, 12）の施錠すべき要所毎に設けられるとともに当該遊技設備（12, …, 12）毎に固有解錠権情報（30a）が各々予め設定されている電子錠手段（30）と、各遊技設備（12, …, 12）毎に設けられ、表示した文字（22a）の発声を促すとともに当該発声された文字（23b）の声紋と予め登録してある声紋との比較を実行し、当該発声声紋と当該登録声紋とが一致したときに当該登録声紋に応じて前記電子錠手段（30）の解錠権（25a）を設定するとともに当該解錠権（25a）を付加した登録声紋解錠権情報（25b）を生成する声紋チェック手段（20）と、前記遊技場（10）内に設けられ、前記電子錠手段（30）の解錠要求（25c）である前記登録声紋解錠権情報（25b）を受けた場合に、当該解錠要求（25c）を受けた電子錠手段（30）に予め設定されている前記固有解錠権情報（30a）と当該登録声紋解錠権情報（25b）との比較を実行し、当該固有解錠権情報（30a）と当該登録声紋解錠権情報（25b）とが一致したときに当該解錠要求（25c）を受けた電子錠手段（30）の解錠の制御を実行する電子錠管理手段（32）と、を備えて成ることを特徴とするセキュリティ管理装置（14）。

【0012】[2] 項 前記声紋チェック手段（20）は、前記表示する文字を所定の規則に基づいて選択して発声文字データ（21a）を生成する発声文字管理部（21）と、前記発声文字データ（21a）を受けて、

当該発声を促す文字を表示する表示部（22）と、前記文字の発声を受けて、前記発声された文字（23b）の声紋の声紋分析を実行して発声声紋データ（23a）を生成する発声声紋管理部（23）と、前記発声声紋データ（23a）と前記登録声紋データ（20a）との比較を実行する声紋チェック部（24）と、前記発生声紋データと前記登録声紋データ（20a）とが一致した場合に、当該登録声紋データ（20a）に応じて前記解錠権（25a）を設定するとともに当該解錠権（25a）を付加した前記登録声紋解錠権情報（25b）を生成するアクセス権付与部（25）と、を備えて成ることを特徴とする[1]項に記載のセキュリティ管理装置（14）。

【0013】[3] 項 前記発声文字管理部（21）は、表示する文字をランダムに選択して前記発声文字データ（21a）を生成する、ことを特徴とする[2]項に記載のセキュリティ管理装置（14）。

#### 【0014】

【作用】本発明におけるセキュリティ管理装置（14）は、機械錠手段に代えて電子錠手段を用い、さらにLoginまたはPassword応答制御に代えて声紋チェックに基づく解錠権に応じて電子錠手段（30）の解錠の制御を実行することができる。

【0015】これにより、遊技場（10）を構成する遊技設備（12, …, 12）への不正アクセス（例えば、遊技設備（12, …, 12）の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができる。

【0016】更に詳しく本発明のセキュリティ管理装置（14）の作用について説明する。遊技場（10）を構成する各遊技設備（12, …, 12）の施錠すべき要所毎に設けられた電子錠手段（30）には、遊技設備（12, …, 12）毎の固有解錠権情報（30a）が各々予め設定されている。

【0017】つまり、鍵と鍵穴式のような機械式一致判定機構による錠手段（機械錠手段）に代えて、声紋チェックに基づく解錠権（25a）に応じて解錠制御される電子錠手段（30）を用い、錠手段（ロック機構）毎の各々専用鍵および錠手段の種類だけの専用鍵を不要とすることにより、遊技設備（12, …, 12）への不正アクセス（例えば、遊技設備（12, …, 12）の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置（14）を実現できる。

【0018】さらに、遊技設備（12, …, 12）に保守整備が必要となった際、合致する専用鍵を一々探し出すことに代えて、声紋チェックによる遊技設備（12, …, 12）の解錠制御が可能となることにより、遊技設備（12, …, 12）への不正アクセス（例えば、遊技設備（12, …, 12）の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができる。

できるセキュリティ管理装置（14）を実現できる。さらに、遊技設備（12, …, 12）の保守整備における過大な労力および時間などの冗費を節減できるセキュリティ管理装置（14）を実現できる。

【0019】各遊技設備（12, …, 12）毎に設けられた声紋チェック手段（20）は、表示した文字（22a）の発声を促すとともに当該発声された文字（23b）の声紋と予め登録してある声紋との比較を実行し、当該発生声紋と当該登録声紋とが一致した場合に当該登録声紋に応じて電子錠手段（30）の解錠権（25a）を設定するとともに当該解錠権（25a）を付加した登録声紋解錠権情報（25b）を生成する。

【0020】更に詳しく本発明の声紋チェック手段（20）の作用について説明する。遊技設備（12, …, 12）に保守整備が必要となり、その旨の要求命令を受けた際、発声文字管理部（21）が、表示する文字を所定の規則に基づいて選択して発声文字データ（21a）を生成する。

【0021】また、発声文字管理部（21）は、表示する文字をランダムに選択して発声文字データ（21a）を生成することもできる。

【0022】発声文字データ（21a）を受けてたとき、表示部（22）が、当該発声を促す文字を表示する。

【0023】文字の発声を受けたとき、発声声紋管理部（23）が、発声された文字（23b）の声紋の声紋分析を実行して発声声紋データ（23a）を生成する。

【0024】発声声紋データ（23a）を受けたとき、声紋チェック部（24）は、発声声紋データ（23a）と登録声紋のデータとの比較を実行する。

【0025】声紋チェック部（24）における発声声紋データ（23a）と登録声紋のデータとの比較の結果、発生声紋データと登録声紋データ（20a）とが一致した場合に、アクセス権付与部（25）が、当該登録声紋データ（20a）に応じて解錠権（25a）を設定するとともに、当該解錠権（25a）を付加した登録声紋解錠権情報（25b）を生成する。

【0026】つまり、鍵と鍵穴式のような機械式一致判定機構によるの錠手段（機械錠手段）に代えて、声紋チェックに基づく解錠権（25a）に応じて解錠制御される電子錠手段（30）を用いるので、専用鍵の紛失、盗取、または模造を防止することが可能となることにより、遊技設備（12, …, 12）への不正アクセス（例えば、遊技設備（12, …, 12）の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置（14）を実現できる。

【0027】さらに、多種類の専用鍵を、紛失、盗取または模造されないように保管しておくための過大な労力および時間などの冗費を節減できるセキュリティ管理装

置（14）を実現できる。

【0028】電子錠手段（30）の解錠要求（25c）である登録声紋解錠権情報（25b）を声紋チェック手段（20）から受けた場合に、電子錠管理手段（32）が、当該解錠要求（25c）を受けた電子錠手段（30）に予め設定されている固有解錠権情報（30a）と当該登録声紋解錠権情報（25b）との比較を実行する。

【0029】比較の結果、当該固有解錠権情報（30a）と当該登録声紋解錠権情報（25b）とが一致したときに、電子錠管理手段（32）は、当該解錠要求（25c）を受けた電子錠手段（30）の解錠の制御を実行する。

【0030】つまり、LoginまたはPassword応答制御に代えて声紋チェックに基づく解錠権（25a）に応じて電子錠手段（30）の解錠の制御を実行することにより、遊技設備（12, …, 12）内への侵入やハッキングが難しくなるので、遊技設備（12, …, 12）への不正アクセス（例えば、遊技設備（12, …, 12）の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置（14）を実現できる。

【0031】さらに、定期的にLoginネームやPasswordを変更必要がなく、高い機密性の保持性が実現できるので、遊技設備（12, …, 12）への不正アクセス（例えば、遊技設備（12, …, 12）の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置（14）を実現できる。

【0032】

【実施例】以下、図面に基づき本発明の一実施例を説明する。図1は本発明の一実施例に係るセキュリティ管理装置14の機能ブロック図であら、図2は本発明の一実施例に係るセキュリティ管理装置14に装置された声紋チェック手段20の機能ブロック図である。

【0033】本実施例におけるセキュリティ管理装置14は、機械錠手段に代えて電子錠手段を用い、さらにLoginまたはPassword応答制御に代えて声紋チェックに基づく解錠権に応じて電子錠手段30の解錠の制御を実行して、遊技場10を構成する遊技設備12, …, 12への不正アクセスを防止するものであり、特に、遊技盤面上に遊技玉を打出して遊技玉の入賞を競うパチンコ遊技機、遊技玉の貸出しを実行するための遊技媒体貸出装置、入賞玉の計数を実行するための賞出媒体計数器等のパチンコ遊技設備、およびこれらのパチンコ遊技設備の統括的な管理を実行するためのパチンコ遊技場管理装置等から構成されるパチンコ遊技場10において、これらの遊技設備12, …, 12への不正アクセスを防止するためものであって、図1に示すように、遊技場10と遊技設備12, …, 12とセキュリティ管理

装置14と声紋チェック手段20と電子錠手段30と電子錠管理手段32とを備えて成る。

【0034】更に詳しく本実施例の構成について説明する。本実施例の遊技機の遊技場10と遊技設備12, ..., 12とセキュリティ管理装置14と声紋チェック手段20と電子錠手段30と電子錠管理手段32とは、マイクロプロセッサーをベースとしたコンピュータを用いて制御を実現している。また、マイクロプロセッサーは、システムバス接続されている。

【0035】同様に、発声文字管理部21と表示部22と発声声紋管理部23と発声された文字23bと声紋チェック部24とアクセス権付与部25とは、マイクロプロセッサーをベースとしたコンピュータを用いて制御を実現している。また、マイクロプロセッサーは、システムバス接続されている。

【0036】遊技場10の遊技管理情報、遊技設備12, ..., 12の遊技管理情報、登録声紋データ20a、発声文字データ21a、表示した文字22aの情報、発声声紋データ23a、発声された文字23bの情報、解錠権25aの情報、登録声紋解錠権情報25b、解錠要求25cの情報、固有解錠権情報30a、等のデータの伝送は、コンピュータのシステムバスを介して実行される。またイーサネットバス、G P-I Bバス、R S 23 2 Cバス、S 1 0 0 バスまたはセントロニクスバス等のバス構造を用いたときは、各々に該当する所定の通信プロトコルに準拠してデータの伝送が実行される。

【0037】制御基盤12aはパチンコ遊技設備12, ..., 12に内設され、パチンコ遊技制御プログラムおよびパチンコ遊技制御情報が記録されパチンコ遊技の制御を実行するパチンコ遊技制御部13は制御基盤12aに実装されて成る。

【0038】パチンコ遊技制御プログラムおよびパチンコ遊技制御情報の記録保持は、マイクロプロセッサーとシステムバスを介して接続されたRAM、ROM、磁気記録媒体、磁気光学記録媒体等の記録媒体によって実現可能である。

【0039】パチンコ遊技制御プログラムおよびパチンコ遊技制御情報はマイクロプロセッサーが実行可能なソフトウェアにより実現している。パチンコ遊技制御プログラムおよびパチンコ遊技制御情報は記録媒体に保存されており、マイクロプロセッサーのコマンドによって読み出されたり、変更されたりできるものである。

【0040】電子錠手段30は、遊技場10を構成する各遊技設備12, ..., 12の施錠すべき要所毎に設けられ、さらに電子錠管理手段32に接続されて成り、当該遊技設備12, ..., 12毎に固有解錠権情報30aが各々予め設定されている。

【0041】声紋チェック手段20は、各遊技設備12, ..., 12毎に設けられ、表示した文字22aの発声を促すとともに当該発声された文字23bの声紋と予め

登録してある声紋との比較を実行し、当該発声声紋と当該登録声紋とが一致した場合に当該登録声紋に応じて電子錠手段30の解錠権25aを設定するとともに当該解錠権25aを付加した登録声紋解錠権情報25bを生成するよう、電子錠管理手段32に接続されて成る。

【0042】電子錠管理手段32は、遊技場10内に設けられ、電子錠手段30の解錠要求25cである登録声紋解錠権情報25bを受けた場合に、当該解錠要求25cを受けた電子錠手段30に予め設定されている固有解錠権情報30aと当該登録声紋解錠権情報25bとの比較を実行し、当該固有解錠権情報30aと当該登録声紋解錠権情報25bとが一致したときに当該解錠要求25cを受けた電子錠手段30の解錠の制御を実行するよう、声紋チェック手段20と電子錠手段30とに接続されて成る。

【0043】声紋チェック手段20は、図2に示すように、発声文字管理部21と表示部22と発声声紋管理部23と発声された文字23bと声紋チェック部24とアクセス権付与部25とを備えて成る。

【0044】発声文字管理部21は、表示する文字を所定の規則に基づいて選択して発声文字データ21aを生成するよう、表示部22に接続されて成る。本実施例では、ルックアップテーブルに予め登録された記号列を用いることができる。

【0045】また、発声文字管理部21は、表示する文字をランダムに選択して発声文字データ21aを生成するよう、表示部22に接続されていてもよい。本実施例では、自動的に乱数発生させた記号列を用いることができる。

【0046】表示部22は、発声文字管理部21から発声文字データ21aを受けて、当該発声を促す文字を表示するよう、発声文字管理部21に接続されて成る。本実施例の表示部22は、C R T表示デバイス、液晶表示デバイス、プラズマ表示デバイス、E L表示デバイス等を用いて実現できる。

【0047】発声声紋管理部23は、表示部22に表示された文字の発声を受けて、発声された文字23bの声紋の声紋分析を実行して発声声紋データ23aを生成するよう、声紋チェック部24に接続されて成る。本実施例の発声声紋管理部23は、表示部22に表示された文字の発声をスピーカーを用いて受信している。

【0048】声紋チェック部24は、発声声紋管理部23が生成した発声声紋データ23aと登録声紋データ20aとの比較を実行するよう、発声声紋管理部23とアクセス権付与部25とに接続されて成る。

【0049】アクセス権付与部25は、発生声紋データと登録声紋データ20aとが一致した場合に、当該登録声紋データ20aに応じて解錠権25aを設定するとともに当該解錠権25aを付加した登録声紋解錠権情報25bを生成するよう、声紋チェック部24と電子錠管理

手段32とに接続されて成る。

【0050】次に作用を説明する。本実施例におけるセキュリティ管理装置14は、遊技盤面上に遊技玉を打出して遊技玉の入賞を競うパチンコ遊技機、遊技玉の貸出しを実行するための遊技媒体貸出装置、入賞玉の計数を実行するための賞出媒体計数器等のパチンコ遊技設備、およびこれらのパチンコ遊技設備の統括的な管理を実行するためのパチンコ遊技場管理装置等から構成されるパチンコ遊技場10において、機械錠手段に代えて電子錠手段を用い、さらにLoginまたはPassword応答制御に代えて声紋チェックに基づく解錠権に応じて、これらの遊技設備12, …, 12の電子錠手段30の解錠の制御を実行することができる。

【0051】これにより、遊技場10を構成する遊技設備12, …, 12への不正アクセス（例えば、遊技設備12, …, 12の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができる。

【0052】更に詳しく本実施例のセキュリティ管理装置14の作用について説明する。遊技場10の遊技管理情報、遊技設備12, …, 12の遊技管理情報、登録声紋データ20a、発声文字データ21a、表示した文字22aの情報、発声声紋データ23a、発声された文字23bの情報、解錠権25aの情報、登録声紋解錠権情報25b、解錠要求25cの情報、固有解錠権情報30a、等のデータの伝送は、コンピュータのシステムバスを介して実行される。またイーサネットバス、GP-Iバス、RS232Cバス、S100バスまたはセントロニクスバス等のバス構造を用いたときは、各々に該当する所定の通信プロトコルに準拠してデータの伝送が実行される。

【0053】パチンコ遊技設備12, …, 12上に実装されたパチンコ遊技制御基盤12aは、パチンコ遊技制御プログラムおよびパチンコ遊技制御情報が記録されている。なお、パチンコ遊技制御プログラムおよびパチンコ遊技制御情報は、パチンコ遊技制御基盤12aに実装されたROMに記録されることが多い。

【0054】パチンコ遊技は、パチンコ遊技制御プログラムおよびパチンコ遊技制御情報に基づいて進行される。

【0055】本実施例におけるパチンコ遊技設備12, …, 12である遊技盤面上に遊技玉を打出して遊技玉の入賞を競うパチンコ遊技機に装置された制御基板12a、パチンコ遊技玉の入賞に応じて生成されるパチンコ遊技結果情報に応じた付与価値を与える（つまり、入賞玉（出玉）の払出し）パチンコ遊技の制御を実行できる。

【0056】パチンコ遊技制御プログラムおよびパチンコ遊技制御情報の記録保持は、マイクロプロセッサーとシステムバスを介して接続されたRAM、ROM、磁気記録媒体、磁気光学記録媒体等の記録媒体によって実現

可能である。

【0057】パチンコ遊技制御プログラムおよびパチンコ遊技制御情報はマイクロプロセッサーが実行可能なソフトウェアにより実現している。パチンコ遊技制御プログラムおよびパチンコ遊技制御情報は記録媒体に保存されており、マイクロプロセッサーのコマンドによって読み出されたり、変更されたりできる。

【0058】本実施例の制御基板12aに用いるパチンコ遊技結果情報とは、例えば、持玉計数器（ジェットカウンタ）（図示せず）からの出玉数情報、特定入賞口（チャッカー）、可変入賞口（V入賞口、通常入賞口）、電動チューリップ、役物（可変表示手段）へのパチンコ遊技玉の入賞回数、入賞順序、入賞タイミング等を意味する。

【0059】また、本実施例の制御基板12aに用いるパチンコ遊技制御情報とは、例えば、入賞時の出玉数率、大当たりパチンコ遊技確率、入賞確率、賞球数、連チャン確立、平均出玉数、等を意味する。

【0060】遊技場10を構成する各遊技設備12, …, 12の施錠すべき所毎に設けられた電子錠手段30には、遊技設備12, …, 12毎の固有解錠権情報30aが各々予め設定されている。

【0061】つまり、鍵と鍵穴式のような機械式一致判定機構による錠手段機械錠手段に代えて、声紋チェックに基づく解錠権25aに応じて解錠制御される電子錠手段30を用い、錠手段ロック機構毎の各々専用鍵および錠手段の種類だけの専用鍵を不要とすることにより、遊技設備12, …, 12への不正アクセス（例えば、遊技設備12, …, 12の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置14を実現できる。

【0062】さらに、遊技設備12, …, 12に保守整備が必要となった際、合致する専用鍵を一々探し出すことに代えて、声紋チェックによる遊技設備12, …, 12の解錠制御が可能となることにより、遊技設備12, …, 12への不正アクセス（例えば、遊技設備12, …, 12の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置14を実現できる。さらに、遊技設備12, …, 12の保守整備における過大な労力および時間などの冗費を節減できるセキュリティ管理装置14を実現できる。

【0063】各遊技設備12, …, 12毎に設けられた声紋チェック手段20は、表示した文字22aの発声を促すとともに当該発声された文字23bの声紋と予め登録してある声紋との比較を実行し、当該発生声紋と当該登録声紋とが一致した場合に当該登録声紋に応じて電子錠手段30の解錠権25aを設定するとともに当該解錠権25aを付加した登録声紋解錠権情報25bを生成する。

【0064】更に詳しく本実施例の声紋チェック手段20の作用について説明する。遊技設備12, …, 12に保守整備が必要となり、その旨の要求命令を受けた際、発声文字管理部21が、表示する文字を所定の規則に基づいて選択して発声文字データ21aを生成する。

【0065】また、発声文字管理部21は、表示する文字をランダムに選択して発声文字データ21aを生成することもできる。

【0066】発声文字管理部21が表示する文字は、予めルックアップテーブルに登録しておいた記号列であったり、自動的に乱数発生させた記号列である。

【0067】発声文字データ21aを受けてたとき、表示部22が、当該発声を促す文字を表示する（例えば、図2に示す「エース」）。

【0068】文字の発声を受けたとき、発声声紋管理部23が、発声された文字23bの声紋（例えば、図2に示す「エ」, 「一」, 「ス」）の声紋分析を実行して発声声紋データ23aを生成する。

【0069】本実施例では、周波数分析による声紋分析を実行しているが、特にこれに限定されるものではなく、音声分析分野で用いられている種々の音声分析の手法を用いることが出来る。

【0070】発声声紋データ23aを受けたとき、声紋チェック部24は、発声声紋データ23aと登録声紋のデータとの比較を実行する。

【0071】声紋チェック部24における発声声紋データ23aと登録声紋のデータとの比較の結果、発声声紋データと登録声紋データ20aとが一致した場合に、アクセス権付与部25が、当該登録声紋データ20aに応じて解錠権25aを設定するとともに、当該解錠権25aを附加した登録声紋解錠権情報25bを生成する。

【0072】つまり、鍵と鍵穴式のような機械式一致判定機構によるの錠手段機械錠手段に代えて、声紋チェックに基づく解錠権25aに応じて解錠制御される電子錠手段30を用いるので、専用鍵の紛失、盗取、または模造を防止することが可能となることにより、遊技設備12, …, 12への不正アクセス（例えば、遊技設備12, …, 12の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置14を実現できる。

【0073】さらに、多種類の専用鍵を、紛失、盗取または模造されないように保管しておくための過大な労力および時間などの冗費を節減できるセキュリティ管理装置14を実現できる。

【0074】電子錠手段30の解錠要求25cである登録声紋解錠権情報25bを声紋チェック手段20から受けた場合に、電子錠管理手段32が、当該解錠要求25cを受けた電子錠手段30に予め設定されている固有解錠権情報30aと当該登録声紋解錠権情報25bとの比較を実行する。

【0075】比較の結果、当該固有解錠権情報30aと当該登録声紋解錠権情報25bとが一致したときに、電子錠管理手段32は、当該解錠要求25cを受けた電子錠手段30の解錠の制御を実行する。

【0076】つまり、LoginまたはPassword応答制御に代えて声紋チェックに基づく解錠権25aに応じて電子錠手段30の解錠の制御を実行することにより、遊技設備12, …, 12内への侵入やハッキングが難しくなるので、遊技設備12, …, 12への不正アクセス（例えば、遊技設備12, …, 12の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置14を実現できる。

【0077】さらに、定期的にLoginネームやPasswordを変更必要がなく、高い機密性の保持性が実現できるので、遊技設備12, …, 12への不正アクセス（例えば、遊技設備12, …, 12の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置14を実現できる。

#### 【0078】

【発明の効果】本発明にかかるセキュリティ管理装置によれば、鍵と鍵穴式のような機械式一致判定機構によるの錠手段（機械錠手段）に代えて、声紋チェックに基づく解錠権に応じて解錠制御される電子錠手段を用い、錠手段（ロック機構）毎の各々専用鍵および錠手段の種類だけの専用鍵を不要とすることにより、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができる。

【0079】さらに、遊技設備に保守整備が必要となった際、合致する専用鍵を一々探し出すことに代えて、声紋チェックによる遊技設備の解錠制御が可能となることにより、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置を実現できる。さらに、遊技設備の保守整備における過大な労力および時間などの冗費を節減できる。

【0080】さらに、鍵と鍵穴式のような機械式一致判定機構によるの錠手段（機械錠手段）に代えて、声紋チェックに基づく解錠権に応じて解錠制御される電子錠手段を用いるので、専用鍵の紛失、盗取、または模造を防止することが可能となることにより、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができるセキュリティ管理装置を実現できる。さらに、多種類の専用鍵を、紛失、盗取または模造されないように保管しておくための過大な労力および時間などの冗費を節減できる。

【0081】また、LoginまたはPassword

13

応答制御に代えて声紋チェックに基づく解錠権に応じて電子錠手段の解錠の制御を実行することにより、遊技設備内への侵入やハッキングが難しくなるので、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができる。

【0082】さらに、定期的にLog inネームやPasswordを変更必要がなく、高い機密性の保持性が実現できるので、遊技設備への不正アクセス（例えば、遊技設備の制御基板の不正すり替えや改造ROM（裏ROM）への不正交換）を防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施例に係るセキュリティ管理装置の機能ブロック図である。

【図2】本発明の一実施例に係るセキュリティ管理装置に装置された声紋チェック手段の機能ブロック図である。

【符号の説明】

10 …遊技場

12, …, 12 …遊技設備

14

12a, …, 12a …制御基盤

14 …セキュリティ管理装置

20 …声紋チェック手段

20a …登録声紋データ

21 …発声文字管理部

21a …発声文字データ

22 …表示部

22a …表示した文字

23 …発声声紋管理部

10

23a …発声声紋データ

23b …発声された文字

24 …声紋チェック部

25 …アクセス権付与部

25a …解錠権

25b …登録声紋解錠権情報

25c …解錠要求

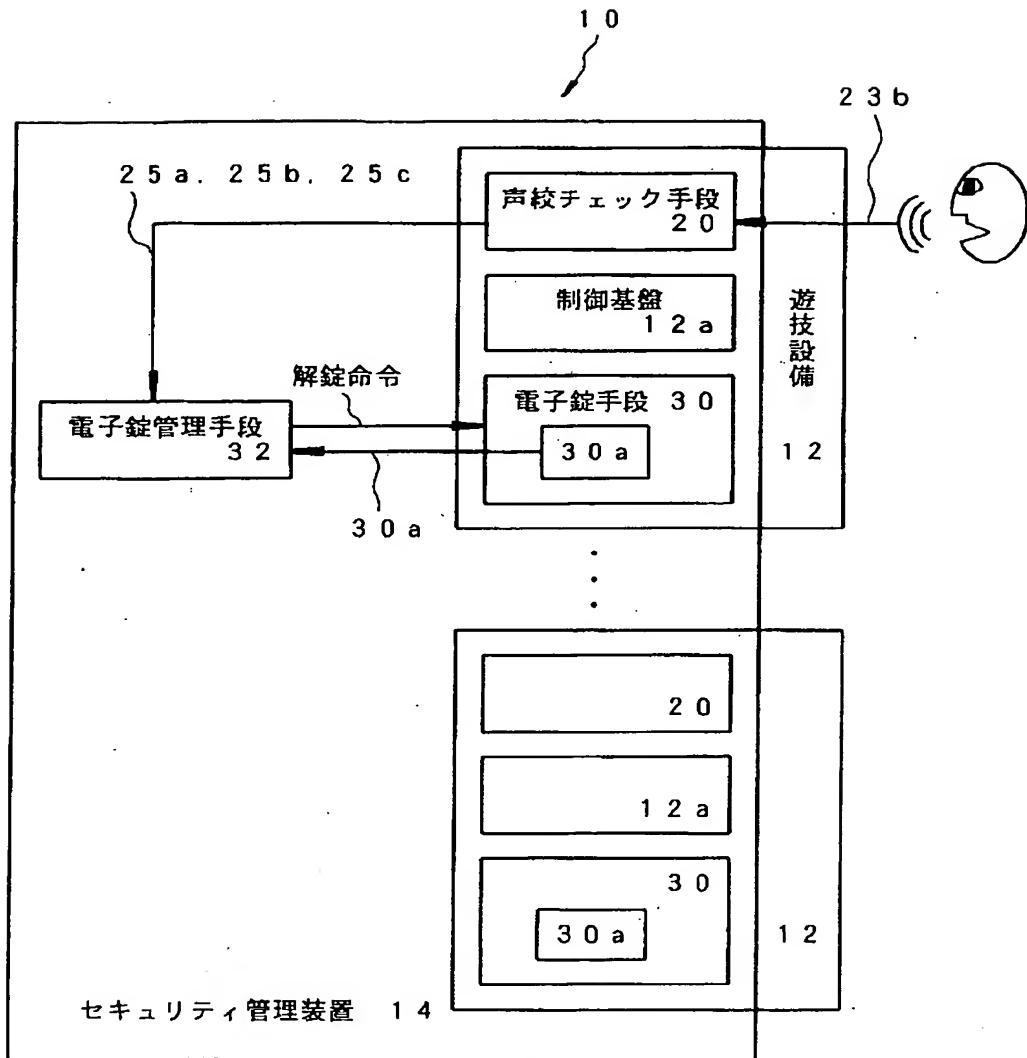
30 …電子錠手段

30a …固有解錠権情報

32 …電子錠管理手段

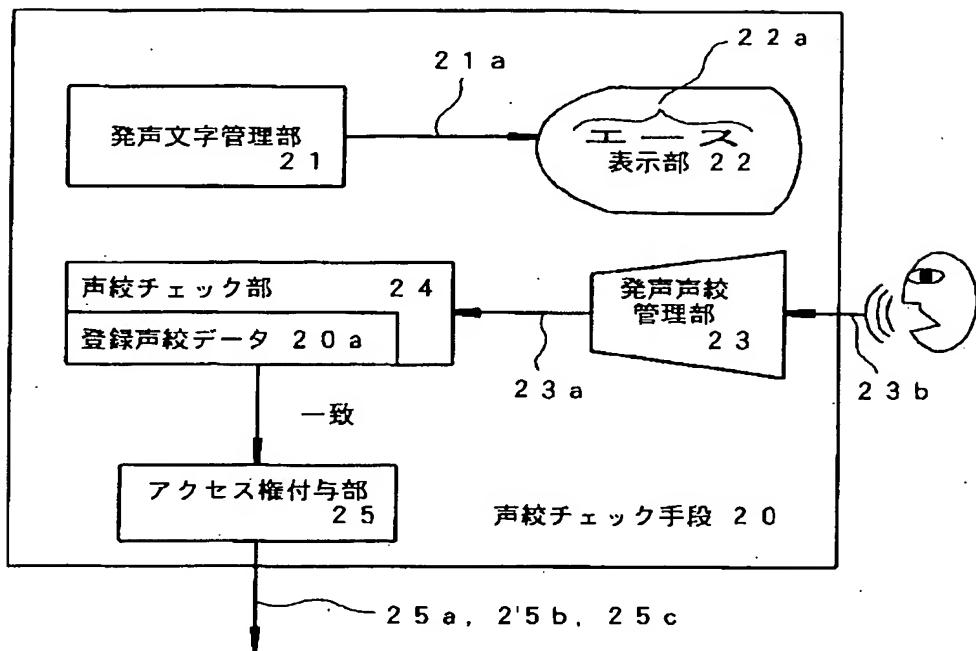
20

【図1】



- 10 … 遊技場
- 12 a, …, 12 a … 制御基盤
- 14 … セキュリティ管理装置
- 23 b … 発声された文字
- 25 a … 解錠権
- 25 b … 登録声紋解錠権情報
- 25 c … 解錠要求
- 30 a … 固有解錠権情報

【図2】



- 20a … 登録声紋データ
- 21a … 発声文字データ
- 22a … 表示した文字
- 23a … 発声声紋データ
- 23b … 発声された文字
- 25a … 解錠権
- 25b … 登録声紋解錠権情報
- 25c … 解錠要求